Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (previously presented) A security device for installation at a node of a digital network, said security device comprising:

a security/encryption engine for providing user transparent communications to another node of said digital network;

a programmed data processor including embedded security policy manager functions for detecting communications which include characteristics which differ from characteristics of normal usage and sending an alarm to said security/encryption engine for communication to another node as said user transparent communications and for responding to user transparent communications from another node of said digital network to control routing of communications in said digital network; and

a communication module for isolating a node by selecting from among redundant communication paths in said digital network.

2. (previously presented) A security device as recited in claim 1, further including a memory for storing information corresponding to said user transparent communication.

3. (original) A security device as recited in claim 1, wherein said routing of communications isolates a node of said digital network.

4. (original) A security device as recited in claim 3, wherein said control of communications to isolate a node of said digital network is performed in real time.

5. (original) A security device as recited in claim 1, wherein said node and said another node are hierarchically arranged locally in said digital network.

6. (original) A security device as recited in claim 1, further including means for defining a secure session between said node and said another node.

7. (original) A security device as recited in claim 6, wherein said means for defining a secure session includes means for transmitting information corresponding to one of an authenticated user and an identification of a communicating node.

8. (original) A security device as recited in claim 1, wherein said characteristics which differ from characteristics of normal usage are characteristics of a potential attack.

9. (original) A security device as recited in claim 1, wherein said characteristics which differ from characteristics of normal usage correspond to a fault at a node or link of said digital network.

10. (original) A security device as recited in claim 1 wherein said programmed data processor includes a manager object and at least one managed object corresponding to each connected node.

11. (previously presented) A digital network comprising

at least two locking devices at each of a plurality of nodes of said digital network,

a security policy manager device for detecting network communications or activity having some characteristics different from characteristics of normal usage and providing a signal to another network node, and

means responsive to a user transparent signal from another node for controlling said at least two locking devices to isolate a node by selecting redundant communication paths in said digital network to maintain network communications between other network nodes.

12. (original) A digital network as recited in claim 11, further including a memory for storing information corresponding to said user transparent communication,

13. (original) A digital network as recited in claim 11, wherein said control of said locking devices to isolate a node of said digital network is performed in real time.

14. (original) A digital network as recited in claim 11, wherein said node and said another node are hierarchically arranged locally in said digital network.

15. (original) A digital network as recited in claim 11, further including means for defining a secure session between said node and said another node.

16. (original) A digital network as recited in claim 15, wherein said means for defining a secure session includes means for transmitting information corresponding to one of an authenticated user and an identification of a communicating node.

17. (original) A digital network as recited in claim 11, wherein said characteristics which differ from characteristics of normal usage are characteristics of a potential attack.

18. (original) A digital network as recited in claim 11, wherein said characteristics of normal usage correspond to a fault at a node or link of said digital network.

19. (original) A digital network as recited in claim 11 wherein said programmed data processor includes a manager object and at least one managed object corresponding to each connected node.

20. (previously presented) A method of operating a digital network including the steps of:

detecting communications having characteristics differing from characteristics of normal usage at a node of said digital network;

communicating a user transparent signal to another node responsive to said detecting step;

controlling communications at said node from said another node with a user transparent signal;

isolating said node from said network by selecting from among redundant communication paths in said digital network to encapsulate said communications having characteristics differing from normal usage; and

routing other communications in said digital network through redundant links between nodes of said digital network.

21. (canceled).

22. (original) A method as recited in claim 20, wherein said detecting step is performed by a managed object at a node of said digital network and said controlling step is performed responsive to a managed object at said another node of said digital network.

23. (original) A method as recited in claim 20 wherein said detecting, communicating and controlling steps are performed in substantially real time.

24. (original) A method as recited in claim 20, including a further step of defining a secure session between a plurality of pairs of connected nodes in a communication path in said digital network.

25. (currently amended) A security device for installation at a node of a digital network, said security device comprising:

a security engine for providing user transparent communications to another node of said digital network;

at least two locking devices, wherein each locking device is coupled to the other locking devices and the security engine, and each locking device is configured to communicate with the other locking devices and with the security engine and to interrupt communication to at least one other node of said digital network; and

a programmed data processor including a memory to store data corresponding to said user communications and to store an embedded security policy manager and a manager object and at least one managed object, wherein the managed object is configured to detect communications at a first node having a characteristic which differs from a normal usage characteristic and to send an alarm through the manager object to said security engine for communication to a managed object of a second node, the managed object corresponding to said first node, as said user transparent communications and for responding to user transparent communications from said second node of said digital network and controlling of routing of communications in said digital network.

26. (previously presented) A security device as recited in claim 25, further comprising a first network port controllably coupled to the security engine and a second network port controllably coupled to the security engine.

27. (previously presented) A security device as recited in claim 26, wherein said controlling of routing of communications includes isolating a node of said digital network by selectively controlling one of the locking devices such that communication with the

node to be isolated is restricted.

28. (previously presented) A security device as recited in claim 27, wherein said isolating a node of said digital network is performed in real time.

29. (previously presented) A security device for installation at a node of a digital network, said security device comprising:

a security engine for providing user transparent communications to another node of said digital network;

at least two locking devices, wherein each locking device is coupled to the other locking devices and the security engine, and each locking device is configured to communicate with the other locking devices and with the security engine; and

a programmed data processor including a memory to store data corresponding to said user communications and to store an embedded security policy manager and a manager object and at least one managed object, wherein the managed object is configured to detect communications at a first node having a characteristic which differs from a normal usage characteristic and to send an alarm through the manager object to said security engine for communication to a managed object of a second node, the managed object corresponding to said first node, as said user transparent communications and for responding to user transparent communications from said second node of said digital network and controlling of routing of communications in said digital network wherein said first node and said second node are hierarchically arranged locally in said digital network and,arranged to provide redundant connections between nodes at different

hierarchical levels.

30. (previously presented) A security device as recited in claim 25, further including a secure session object configured to establish a secure session between said first node and said second node.

31. (previously presented) A security device as recited in claim 30 wherein said secure session object includes a communication module to transmit information corresponding to one of an authenticated user and an identification of a communicating node, wherein the identification of the communicating node can be used to isolate nodes corresponding to the secure session.

32. (previously presented) A security device as recited in claim 25, wherein said characteristic differing from said normal usage characteristic is a potential attack characteristic.

33. (previously presented) A security device as recited in claim 25, wherein said characteristic differing from said normal usage characteristic corresponds to a fault at a node or link of said digital network.

34. (previously presented) A security device as recited in claim 25, wherein said manager object manages said managed object, and wherein each managed object corresponds to a connected node.

35. (previously presented) A digital network for active intrusion resistance, said digital network comprising:

a plurality of nodes arranged in a tiered hierarchy, each node including

at least two locking devices;

a security policy manager device for detecting network communications or activity having a characteristic different from a normal usage characteristic and providing a signal to other network nodes; and

a communication module responsive to a user transparent signal from another node for controlling said at least two locking devices to isolate a node by selecting from among redundant communication paths in said digital network to maintain network communications between nodes that are not to be isolated and restricting communications with a node to be isolated, whereby the digital network actively resists intrusion by isolating one or more nodes that are determined to have become untrusted.

36. (previously presented) A digital network as recited in claim 35, wherein each node further includes a memory to store data corresponding to said user transparent communications and to store an embedded security policy manager, a manager object, and managed objects corresponding to each connected node.

37. (previously presented) A digital network as recited in claim 35, wherein said controlling of said at least two locking devices to isolate a node of said digital network is performed in real time.

38. (previously presented) A digital network as recited in claim 35, wherein said tiered hierarchy includes redundant connections between nodes at different levels in the hierarchy.

39. (previously presented) A digital network as recited in claim 35, wherein each node further includes a module for defining a secure session between nodes.

40. (previously presented) A digital network as recited in claim 39, wherein said module for defining a secure session includes a portion to transmit information corresponding to one of an authenticated user and an identification of a communicating node, wherein the identification of the communicating node can be used to isolate nodes corresponding to the secure session such that the digital network actively resists intrusion by compartmentalizing untrusted nodes within the secure session.

41. (previously presented) A digital network as recited in claim 35, wherein said characteristic which differs from said normal usage characteristics is a potential attack characteristic.

42. (previously presented) A digital network as recited in claim 35, wherein said characteristic that differs from said normal usage characteristic corresponds to a fault at a node or link of said digital network.

43. (previously presented) A digital network as recited in claim 35, wherein said manager object manages said managed object, and wherein each managed object corresponds to any external node coupled to each node.

44. (previously presented) A method of actively resisting intrusion in a digital network using extensions to an object request broker, said method comprising:

providing object request broker software;

extending the object request broker software to include encryption, intrusion detection, and security policy management and enforcement;

generating a manager object on one or more nodes and at least one managed object on each node;

detecting, with a managed object, a communication having a characteristic differing from a normal usage characteristic at a first node of said digital network, said communication received from a second node of said digital network;

communicating a user transparent signal from a managed object of the first node to a managed object of a third digital network node responsive to said detection; and

controlling communications, through coordinated managed and manager objects, at said first node and said third node to restrict communications from said second node with a user transparent signal.

45. (previously presented) A method as recited in claim 44, wherein said step of controlling communications includes steps of

isolating said second node from said digital network to restrict untrusted communications from the second node from being allowed onto the digital network, and

routing other digital network communications through redundant links between nodes of said digital network so as to bypass and isolate the second node.

46. (previously presented) A method as recited in claim 44, wherein said detecting step is performed by the managed object at the first node of said digital network and said controlling step is performed responsive to the managed object at said third node of said digital network.

47. (previously presented) A method as recited in claim 44, wherein said detecting, communicating and controlling steps are performed in substantially real time.

48. (previously presented) A method as recited in claim 44, including a further step of defining a secure session between a plurality of nodes in a communication path in said digital network, wherein said secure session allows compartmentalization of any untrusted nodes.